AO 106 (Rev. 01/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of New Mexico

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109, as more fully described in Attachment A.	Case No. 15 mr 370

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the _____ District of New Mexico *(identify the person or describe property to be searched and give its location):* The residential property and premises located at the Canyon Vista Apartments, 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109. The building is brown in color and has windows facing the west. Apartment 101 is located on the west side of the building on the bottom floor. "101" is affixed to the entry door.

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: Evidence of, or contraband, fruits of, or other items related to the offense of 18 U.S.C. 2252, Distribution, Receipt, and Possession of visual depictions of minors engaged in sexually explicit conduct, as described in Attachment B incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252, and the application is based on these facts: See attached Affidavit, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Melva Boling, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 6-10-15

Judge's signature

City and state: Albuquerque, NM

Kitan Khalsa, US Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF
The residential property and premises located at 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109
Described in Attachment A
Incorporated herein by reference

AFFIDAVIT OF SPECIAL AGENT MELVA BOLING

I, Melva Boling, being duly sworn, hereby declare and state as follows:

Your Affiant is a Special Agent with the Department of Homeland Security, Homeland Security Investigations, hereafter referred to as HSI, and has been employed by HSI as such since June 2010. Your Affiant is currently assigned to the Assistant Special Agent in Charge, Albuquerque, New Mexico where your Affiant is assigned to investigate individuals involved in the exploitation of minors including violations of Title 18, United States Code, Section 2252. Your Affiant has worked on child pornography and child exploitation investigations and has been trained in the investigation of computer related child exploitation and child pornography cases by the Department of Homeland Security and the Internet Crimes Against Children Task Force. During the investigation of these cases, your Affiant has executed, or participated in the execution of, numerous search warrants and seized evidence of these violations.

Your Affiant successfully completed eleven weeks of Criminal Investigator Training at the Federal Law Enforcement Training Center (FLETC). In addition, your Affiant completed eleven weeks of Special Agent Training with Immigration and Customs Enforcement, also at FLETC. Your Affiant holds a Bachelor's Degree in Oral Communication-Theater from the University of Central Oklahoma.

This affidavit is made in support of an application for a warrant to search the residential property and premises located at 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109 as described in Attachment A, incorporated herein by reference, and to search for, seize and examine items, as more particularly described in Attachment B, incorporated herein by reference.

This affidavit is based upon information your Affiant has gained through investigation, training and experience, as well as information from other law enforcement officers whom your Affiant believes to be reliable. Since this affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known to her concerning this investigation. Your Affiant has set forth only the facts that she believes are necessary to establish probable cause to believe instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Section 2252 are located at the residential property and premises 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109, as more particularly described in Attachment A, incorporated herein by reference, and to

search for, seize and examine items, as more particularly described in Attachment B, incorporated herein by reference.

BACKGROUND AND SUMMARY OF INVESTIGATION

The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The World Wide Web (www) is a functionality of the Internet, which allows users of the Internet to share information.

A growing phenomenon on the Internet is Peer-To-Peer (P2P) file sharing. P2P file sharing programs are a standard way to transfer files from one computer system to another while connected to a network, usually the Internet. P2P file sharing programs allow groups of computers using the same file sharing network and protocols to connect directly to each other to share files. There are several P2P networks currently operating, these include the "ARES network".

Your Affiant knows from training and experience that P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files, of child pornography, include both image and movie files.

Many P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files if they are not sharing files. Typically, settings within these programs control sharing thresholds.

With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, and wireless.

To access the P2P networks, a user first obtains the P2P software, which can be downloaded from the Internet. This software is used exclusively for the purpose of sharing digital files. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to anyone on the world-wide network for download. Most P2P software gives each user a rating based on the number of files he/she is contributing to the network. This rating affects the user's ability to download files. The more files a user is sharing, the greater his/her ability is to download files. This rating system is intended to encourage users to "share" their files, thus propagating the P2P network. However, a user is not required to share files to utilize the P2P network.

A user obtains files by conducting keyword searches of the P2P network. When a user initially logs onto the P2P network, a list of the files that the user is sharing is transmitted to the network. The P2P software then matches files in these file lists to keyword search requests from other users. A user looking to download files simply conducts a keyword search. The results of

the keyword search are displayed and the user then selects file(s) which he/she wants to download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer(s) hosting the file. Once a file has been downloaded, it is stored in the area previously designated by the user and will remain there until moved or deleted. Most of the P2P software applications keep logs of each download event. Frequently, a computer forensic examiner, using these logs, can determine the Internet Protocol ("IP") address from which a particular file was obtained.

Thus, a person interested in sharing child pornography with others in the P2P network, need only place those files in his/her "shared" folder(s). Those child pornography files are then available to all users of the P2P network for download regardless of their physical location. For instance, a person interested in obtaining child pornography can open the P2P application on his/her computer and conduct a keyword search for files using a common child pornography term such as "preteen sex." The keyword search would return results of files being shared on the P2P network that match the term "preteen sex." The user can then select files from the search results and those files can be downloaded directly from the computer(s) sharing those files.

One of the advantages of P2P file sharing is that multiple files may be downloaded in parallel. This means that the user can download more than one file at a time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a user downloading an image file may actually receive parts of the image from multiple computers. This reduces the time it takes to download the file.

P2P networks can only succeed in reassembling the file from different parts if the parts all come from the same original file. Multiple persons sharing one file can deliver different pieces of that file to the local software and the local software can insure that a complete and exact copy can be made from the parts. Use of the software has confirmed that different copies of the same file can be named differently.

P2P networks use “hash values” to insure that two files are exactly the same. A Hash value is a number that uniquely identifies the contents of a file. The value is generated by, applying a mathematical algorithm to a file, which assesses the contents of the file. There are several types of algorithms that can be applied; SHA1, MD5, and MD4 are common algorithms. A hash value is generated by a software program has “hashes” or “evaluates” the contents of the file and generates the unique number identifying the contents of the file.

Hash values are a very reliable method of authenticating files. If the same mathematical algorithm is applied to two files, two hash values will be generated. If the two hash values match, one can conclude, with a great deal of certainty, that the contents of both files are identical.

Files on the BitTorrent network:

- The BitTorrent network is a very popular and publically available P2P file sharing network. Most computers that are part of this network are referred to as “peers” or

"clients". A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

- The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, uTorrent client program, and Vuze client program, among others. These client programs are publically available and typically free P2P client software programs that can be downloaded from the Internet.
- During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading[1]. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as "seeding".
- Files or sets of files are shared on the BitTorrent network via the use of "Torrents". A "Torrent" is typically a small file that *describes* the file(s) to be shared. It is important to note that "Torrent" files do not contain the actual file(s) to be shared, but information about the file(s) to be shared needed to accomplish a download. This information includes things such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1[2]hash value of the set of data describing the file(s) referenced in the "Torrent". This set of data includes the SHA-1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The "info hash" of each "Torrent" uniquely identifies the "Torrent" file on the BitTorrent network. The "Torrent" file may also contain information on how to locate file(s) referenced in the "Torrent" by identifying "Trackers". "Trackers" are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the "Torrent" file. A "Tracker" is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the "Torrent". "Trackers" do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of "Tracker(s)" on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular "Torrent" file. There are many publically available servers on the Internet that provide BitTorrent tracker services.
- In order to locate "Torrent" files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include *isohhunt.com* and the *piratebay.org*. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate "Torrent" files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by "Torrent" files, only the "Torrent" files themselves. Once a "Torrent" file is located on the website that meets a user's

keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file. It is again important to note that the actual file(s) referenced in the "Torrent" are actually obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA-1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent", to include the remote peers/clients Internet Protocol (IP) addresses.

- For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients are located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files. Typically, once the BitTorrent network client has downloaded part of a file or files, it may immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 hash value of that piece which is described in the "Torrent" file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user's computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.
- Law Enforcement can search the BitTorrent network in order to locate individuals sharing previously identified child exploitation material in the same way a user searches this network. To search the network for these known torrents can quickly identify targets in their jurisdiction. Law Enforcement receives this information from "Trackers" about peers/clients on the BitTorrent network recently reporting that they are involved in sharing digital files of known or suspected child pornography, based on "info hash" SHA-1 hash values of torrents. These torrents being searched for are those that have been previously identified by law enforcement as being associated with such files. There are BitTorrent network client programs which allow for single-source downloads from a computer at a single IP address, meaning that an entire file or files are downloaded only from a computer at a single IP address as opposed to obtaining the file from multiple peers/clients on the BitTorrent network. This procedure allows for the detection and investigation of those computers involved in

sharing digital files of known or suspected child pornography on the BitTorrent network.

- During the query and/or downloading process from a suspect BitTorrent network client, certain information may be exchanged between the investigator's BitTorrent client program and the suspect client program they are querying and/or downloading a file from. This information includes 1) the suspect client's IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer. The law enforcement has the ability to log this information.
- The investigation of peer-to-peer file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes against Children Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the sexual exploitation of actual child victims.

A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular Internet connection during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

Even though the P2P network links together computers all over the world and users can download files, it is not possible for one user to send or upload a file to another user of the P2P network. The software is designed only to allow files to be downloaded that have been selected. One does not have the ability to send files from his/her computer to another user's computer without their permission or knowledge. Therefore, it is not possible for one user to send or upload child pornography files to another user's computer without his/her active participation.

Your Affiant knows from training and experience that computers and other devices, which are connected to or previously connected to the Internet, identify each other by an Internet Protocol or IP address. Your Affiant knows that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account and property that uses the IP address to access the Internet.

Your Affiant knows that searching on the peer-to-peer network as described below can result in your Affiant receiving a list of IP addresses identifying locations where a computer has software installed and individual files have been reported as available for trade with a specific digital signature.

Your Affiant knows a records request to an Internet service provider can result in your Affiant receiving a specific address that corresponds with the use of a computer. This address is the most frequent method of locating the actual computer involved in criminal activity.

The returned list of IP addresses can include computers that are likely to be within this jurisdiction. The ability to identify the approximate location of these IP address is provided by IP geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, a recent association between a known child pornography file (based upon MD4 root hash comparison or SHA1) and a computer having a specific IP address (likely to be located within a specific region) can be established.

Once this association has been established, an investigator can attempt to download the file from the associated user or view the contents of the shared directory.

Depending on the associated user configuration and available peer resources a listing of the files being shared may be displayed. In order to obtain this list of files, a direct connection between the computers must occur. This list can be a partial listing of the shared files. The file list can **only** be obtained if the associated peer is connected to the network and running a P2P client at that moment.

By receiving either a file list or portions of a download from a specific IP address the investigator can conclude that a computer, likely to be in this jurisdiction, is running a P2P client and possessing, receiving and/or distributing visual depictions of child pornography.

This investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the Internet Crimes Against Children Task Force Program, Homeland Security Investigations, or the Federal Bureau of Investigation. Many of the officers involved in this effort are using the technology and methods described herein. This methodology has led to the issuance and execution of search warrants around the country resulting in many seizures of child pornography and arrests for possession, distribution and receipt of child pornography.

CURRENT INVESTIGATION

On November 6, 2014, Special Agent (SA) Owen Pena of the New Mexico Attorney General's Office was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **a0bf533648971de2d043d021f55e50419d8f05c9**. This torrent file references 13 files, at least one of which was identified as a file of investigative interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116**, hereinafter referred to as "Suspect Device." The Suspect Device reported it was using BitTorrent client software -BA3300- uTorrent 3.3.

Between November 6, 2014 at 1814 hours MST and November 7, 2014 at 1452 hours MST, SA Pena completed the download of the following 2 files that the device at IP address **174.56.57.116**

was making available. The device at IP Address **174.56.57.116** was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

- **6.jpg** **O52ZHG7QQ3FS74RWNI325S3Y4NX6CX6Z**
- **cap.jpg** **GXMJBUJO526NGXVTZL2ZSXFHK4XHKWSJ**

SA Pena then looked through the file structure of InfoHash: **a0bf533648971de2d043d021f55e50419d8f05c9** and observed that in the folder titled: "LS Dream Issue 6 Secret Place - All Movies". This is where the above listed 2 "Files of Interest" were located, along with multiple other image/video files. Some of these files were complete or incomplete and some could be considered "Child Erotica" and "Child Pornography."

SA Pena reviewed the above listed downloaded .jpg files and they are described as follows:

- **6.jpg (SHA1: O52ZHG7QQ3FS74RWNI325S3Y4NX6CX6Z) (Located Inside Folder: LS Dream Issue 6 Secret Place - All Movies)** This color .jpg image file depicts a screenshot of a web page titled: "Secret Place". The following statements are on this web page: "Don't Restrain Yourself", "No Rules And No Restrictions", "Be Yourself And Follow Your Natural Bent" and "Your Secret Place-Your Little World Of Joy And Satisfaction". The web page depicts two (2) semi-clothed pre-pubescent females standing and posing. The girl's breasts, buttocks and vaginal areas are exposed. One of the girls is posed in a lewd and lascivious manner. These girls appear to be between 7 and 11 years old, due to their body size comparison/ development, none to very slight breast development and no pubic development.

- **cap.jpg (SHA1: GXMJBUJO526NGXVTZL2ZSXFHK4XHKWSJ) (Located Inside Folder: LS Dream Issue 6 Secret Place - All Movies)** This color .jpg image file is a collage of still images of naked pre-pubescent females in outdoor settings and posed in different positions, in various stages of undress. The young girl's breasts, buttocks and vaginal area are exposed. Some of the young girls have their legs spread apart and with the camera zoomed in on their vaginas. Some of the stills could be considered "Child Erotica" and some of the stills can be considered "Child Pornography". These girls appear to be between 7 and 11 years of age, due to their body size comparison/ development, none to very slight breast development and no pubic development.

Possessing and distributing these files does constitute a violation of the Sexual Exploitation of Children federal statue Title 18, United States Code, Section 2252 and all of these files are considered child pornography.

On November 9, 2014, SA Pena was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **1d1ed765e668da435ef02b6cabe6fd762b2b9415**. This torrent file references 831 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116**, hereinafter referred to as "Suspect Device." The Suspect Device reported it was using BitTorrent client software -**BA3300- uTorrent 3.3**.

On November 9, 2014, between 2018 hours and 2342 hours MST, SA Pena successfully completed the download of the following 25 file(s) that the device at IP address **174.56.57.116** was making available. The device at IP Address **174.56.57.116** was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

- **ism-016-011.jpg** **EB3UC43K6WIAT4JYHC6VJ25WHFTHUCYM**
- **ism-016-012.jpg** **3PPVH5654AHZTVI34XSUKUS3KBQUBLGS**
- **ism-016-013.jpg** **3QTCACOCSG6MYJRC6MXRPAPOWJIQCN5J**
- **ism-016-014.jpg** **H23KFVKGR3JKYZOQ3IDOOTPHLXCBR4B5**
- **ism-016-015.jpg** **SATCVTMI7DAHKBX45AIUWOX6AL7NL6OE**
- **ism-016-032.jpg** **VYSSGW7EFGZ2RV72SH3R5YI7NZQ7ZBSU**
- **ism-016-033.jpg** **5BYMXQDI642F3A3N3GPQXOTU7THR7XKR**
- **ism-016-058.jpg** **MVETQILT774GQKHCYZHCAVZHL2QANCCQ**
- **ism-016-071.jpg** **2F64YNPWCLRYERWCAD23RU734GNXCAUN**
- **ism-016-072.jpg** **4RGAW36YV2C66HRP6OAKDVFVYGI52JAT**
- **ism-016-090.jpg** **PXVFFCHVUC5RXYWPHEWU2PMQWJEHUQ6X**
- **gu-037-051.jpg** **UKM3U5EXQDX5WN52KJT7BBBTYHZFVEY4**
- **gu-037-073.jpg** **SKBJN3MI77L542F7E2JIERQRUQ6LBMPZ**
- **gu-037-074.jpg** **AGGVHHOZODO7ROIR6WVKM6NEBFXOC3VU**
- **gu-037-081.jpg** **TGZF6BWU3HFB2CBS6XT7E2P72AVEYPC2**
- **gu-037-083.jpg** **Z42I4DNN2BEJN3YBBZYSHA3ZKINEGKH3**
- **gu-037-087.jpg** **YRHCECFSEURSM5KWDTWYLVZTV3QRVAFQ**
- **ps-018b-001.jpg** **NTA4GMCRJF5HNWM3N6HLNFKDHT7G5SMZ**
- **ps-018b-029.jpg** **IXMOF7F3SJTJZOH7VAS3AXQQVDNDSS7D**
- **touch-001a-031.jpg** **AQMSRSWUGHWE5EZXQC74XBF6OEZUYPXK**
- **touch-001a-032.jpg** **HU7L77BKJUINEX3AGONKU4HKC5GZ6ZGR**
- **touch-001a-033.jpg** **32GXNVYZT4VU5QS2KMXUW6YD64EUS5U4**
- **touch-001a-063.jpg** **WDZV2XVRM3PBQTRRS37XRIQ7X7AMY7TV**
- **touch-001a-101.jpg** **M6BN23FIO5SSIQOWGCZCUO7SYKYKUANI**
- **touch-004b-083.jpg** **M4BDSJCXYE6WCEY7KUGAE3O4W65QAK6D**

SA Pena then looked through the file structure of InfoHash: **1d1ed765e668da435ef02b6cabe6fd762b2b9415** and observed in the folder titled: "Shining Pretties_ Little Pirates, etc LS [8 LS sets]" inside this folder were the following subfolders: "LS Island-03-Midsummer_ism-016," "LS Little Guests 037,", "LS Shining Pretties 018b," "LS Star 014b," "LS Touch 001a," "LS Touch 004b," "LS-Land.issue.01.perfects.lsp-005a," "LS-Land.issue.06.Little.Pirates.lsp-007.by_zic," and multiple Torrent/text files. This is where the above listed 25 "Files of Interest" are located. Some of these files were complete or incomplete and some of the files could be considered "Child Erotica" and "Child Pornography".

SA Pena reviewed the above listed downloaded .jpg files and some are described as follows:

- **ism-016-058.jpg (SHA1: MVETQILT774GQKHCYZHCAVZHL2QANCCQ) (Located Inside Folder: LS Island-03-Midsummer_ism-016)** This color .jpg image file depicts a naked pre-pubescent female standing in an outside setting, leaning against a rock and facing away from the camera. The girl is shown from hips to her upper thigh area, with a multi-colored cloth around her waist. The girl has her legs spread apart and the focal point of the close-up image is her vagina and anus. The girl also has her hand on her buttock, appears to be spreading her buttocks for the camera. In the upper right corner of the image is the logo "LS island". This girl appears to be between 8 and 11 years old, due to her body size comparison/development and no pubic development.

- **gu-037-051.jpg (SHA1: UKM3U5EXQDX5WN52KJT7BBBTYHZFVEY4) (Located Inside Folder: LS Little Guests 037)** This color .jpg image file depicts a naked pre-pubescent female in a studio setting and laying on her right side. The girl is shown from her stomach to her lower thigh area, with a see through green top and beads around her waist. The young girl has her legs spread far apart and with her left leg lifted into the air. The focal point of the close-up image is her vagina and anus. The girl's buttocks are also visible. In the upper right corner of the image are the logos: "LS MODELS.COM" and "http://www.ls-models.com." This girl appears to be between 8 and 11 years of age, due to her body size comparison/development and no pubic development.

- **gu-037-081.jpg (SHA1: TGZF6BWU3HFB2CBS6XT7E2P72AVEYPC2) (Located Inside Folder: LS Little Guests 037)** This color .jpg image file depicts a naked pre-pubescent female in a studio setting, bending over backwards, while on her hands and feet. The girl is shown from her stomach to her lower thigh area. The girl has her legs spread far apart. The focal point of the close-up image is her vagina, and her buttocks are also visible. In the upper right corner of the image are the logos: "LS MODELS.COM" and "http://www.ls-models.com." This girl appears to be between 8 and 11 years of age, due to her body size comparison/development and no pubic development.

Possessing and distributing these files does constitute a violation of the Sexual Exploitation of Children federal statue Title 18, United States Code, Section 2252 and all of these files are considered child pornography.

On November 11, 2014, SA Pena was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **ebac972f542da319c737e96c43bae9d50b3784e3**. This torrent file references 171 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116**, hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software **-BA3300- uTorrent 3.3**.

On November 11, 2014, between 0023 hours and 0122 hours, SA Pena successfully completed the download of the following 35 file(s) that the device at IP address **174.56.57.116** was making

available:. The device at IP Address **174.56.57.116** was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

- **25072003-1124.jpg PRSKQI23C5P5BUHZTDVGPYJ47OMVOYB6**
- **IMG_4142.jpg XS7E6KCSMLMYJRH6BBBVDB7WEUH7OLYA**
- **25072003-1091.jpg 5INRKXD4V3A5IFA5TS6B5KCXCPV3BOWL**
- **Sandra-mix-28.jpg RPNOG5L4ETNPKA3CNKJZJME7XH5D7PNB**
- **ptsc Sandra Teen Model 00011 Nude underwater small pics (1).jpg EAQSYUIEFNVYAWYNGZCEAPK2Z6EFP25I**
- **sandra3.jpg IXM6JMRNBHL3C32DNTSRIK5QEERF3FHM**
- **25072003-1139.jpg EX7C4WBIWI43EDA55Z2JXERE7ZAU3R3O**
- **Sandra-mix-23.jpg AFHR4C7VDD2QE37JE6YSMHD6KJB4RPS7**
- **25072003-1122.jpg 5TJLJHE4QMC5CP3SS2ZSV3QZFGQTZTAY**
- **s23.jpg 7PMXANEQ32B7S4OZCJRFTARUNEG3H4WV**
- **25072003-1105.jpg 53TGKOAWYVJWZZ5DY6V2YFUBUBVQH47F**
- **Sandra-mix-15.jpg YP5SORONGGUGMBIGKYKLDTTW6KDTBTWF**
- **Sandra-mix-17.jpg E4PPNPEZ4FOKF6E3HQLV4BMX5PSMCQRU**
- **25072003-1159.jpg XKJXTAY7U4XQKNZMREGLXUI5OEVELP4K**
- **Sandra-mix-54.jpg CT3SHONPWEMB63HLHAITSPDPETVVHX7D**
- **Sandra-mix-55.jpg 3R4AWM43LUC4ZXH7NZ737L4Y6NGSBK7W**
- **Sandra Teen Model Nude 00017.jpg ZCS7CUC7JTOQY2JN2VQJ6JNTDBRSTVW**
- **1111274542.jpg 6LBHRKBO2VZBCK3XAVZFCOOITWEZSTV5**
- **s20.jpg ICAUEQR7NT2LHW4HAJK5CEFM57XIGXYS**
- **Sandra-mix-16.jpg QXMA2POEKN5V3AO2BGWLWEEOTM23TV56**
- **25072003-1145.jpg ZT4IMGRSDQSVA5YM43D2MQHZDJQLE5U6**
- **25072003-1144.jpg HCX36SNMEQFWW55N4LKPGE2F642MIFO5**
- **SANDRA_MIX_60.jpgHVOVQHDIXW7EUWZMGUYDV7UI3JBVLZIW**
- **Sandra-mix-51.jpg LVOB57PAWQZOMPC6ZZFHHQWKRU5RQBTO**
- **s18.jpg GFW6IREFKRHLKZ5GALAVLMCAHO7KRMU5**
- **25072003-1143.jpg 4D2I2WEKNYT6YZKHOZ2N3BWFELGMESTZ**
- **s21.jpg IGAJKRH7PNLCMKHSGFLIZSIQAVQJ3LV3**
- **s7.jpg HEZWCNGDRAEVWPUXCDE5PQIIGJ77REUB**
- **s17.jpg HBGKFPGYBT56RBRXQHVBUNJGLTTAXBTQ**
- **Sandra nude.jpg TW4SRJ34LATYOZA4JNHKF25OVW7E7FQE**
- **25072003-1146.jpg QGV6YS35734W3Y7ESJE3IQXLBP347IRW**
- **s16.jpg 75YCJYX3YJX4VN4AKJ6AXCJJWQSA6VH5**
- **Sandra-mix-52.jpg PQ42LDC4TRZ24I7VILTKQU5JC4VK7B6O**
- **Sandra-mix-61.jpg I3RWTZ5U63SCJHPI4HXY7HVD5ZNBN7A3**
- **Sandra74_jpg.jpg IK3GY7DGOM6GV3Z36Y7KNNELOLWGLWPY**

SA Pena then looked through the file structure of InfoHash: **ebac972f542da319c737e96c43bae9d50b3784e3** and observed that in the folder titled: "**Sandra Model (Misc nude)**." This is where the above listed 35 "Files of Interest" are located. Some of

these files were complete or incomplete and some of these files could be considered "Child Erotica" and "Child Pornography."

On November 11, 2014, SA Pena was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **ebac972f542da319c737e96c43bae9d50b3784e3**. This torrent file references 171 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116**, hereinafter referred to as "Suspect Device." The Suspect Device reported it was using BitTorrent client software **-BA3300- uTorrent 3.3**.

On November 11, 2014, between 1224 hours and 1719 hours MST, SA Pena successfully completed the download of the following 152 file(s) that the device at IP address **174.56.57.116** was making available:. The device at IP Address **174.56.57.116** was the sole candidate for each download, and each file was downloaded directly from this IP Address.

- **25072003-1185.jpg QKAFGY54RO33VBMP5U6OF54D5XHJO7TT**
- **25072003-1164.jpg RNCTNJ4SOZ2QR4XRURKYSGE5W5MAIDAX**
- **25072003-1155.jpg YODNODK52VTAVF5JC2M5LQUFY7ZDOVGK**
- **25072003-1181.jpg 62H4TLR3C5AGJY2OXLDIO3XR3CZAGA7G**
- **25072003-1165.jpg JC6XJ4RECOBK53WBPWOF6FIK34QWBYO5**
- **16112003-10164.JPGWCXBYJ2AAFZQJFLFEDR5LJRPNJCJ625P**
- **25072003-1184.jpg SRHDDS6JF57FYOEOJRJAJ4NCK2D5Y3UT**
- **25072003-1178.jpg ICPYF62I3QLOZJAANZKUPWKO5LIFEHFF**
- **s19.jpg WAPYWOASKJUCFO4R6QS22WWKY6PWIO7I**
- **25072003-1087.jpg 73NNWJDQRGT5OXZ5LAUA7BGICVFN3CHK**
- **25072003-1128.jpg DFYLJ5OZUIMUZA5QGRVX4PE2APOIM6QC**
- **25072003-1148.jpg 4BORQZZLLAKDYSLPA3VNJIVFF4R2VBUL**
- **25072003-1176.jpg HCM5BBSMEBFRRZV3J54EFEJRVYAKBNX5**
- **25072003-1152.jpg G5EJZDN62CKS5RSPG6BPVJ7GOERX2S6J**
- **25072003-1182.jpg CSR5H66W6MIYHBEVN6BAZPFPRBDSWMIZ**
- **25072003-1126.jpg NYQHJSTE5TVMJJEEBZ6YLCDKTDCWBL5S**
- **25072003-1154.jpg EMFLAZMTVF7QANNSTNOSPRBA4NYFARNZ**
- **25072003-1189.jpg ZBGCPS5654SVJXKHF2FDX4NA33LSNK3A**
- **25072003-1108.jpg H56CS4WIQRH7CQ2L4ZLAVP3N3Q2VHAOM**
- **25072003-1116.jpg T5LV7KRI3KJUPUSRH5IBWMNETTCDTR6U**
- **s3.jpg FAVWX37HDG2I73LDTZQPAXI6BXMMYJZM**
- **25072003-1183.jpg FAVWX37HDG2I73LDTZQPAXI6BXMMYJZM**
- **s15.jpg NK72Z7M7EMQQ2ETZY3OPBT2C3YCE2363**
- **23012005-199.jpg SN7MWFHSD537M4M5QBOGUSXQDILQDEHI**
- **25072003-1115.jpg E2OZJK34B67WJ7G237MNEVNV752VWS4A**
- **16112003-10086.jpg XKOWSXDJK72HIAH6DKFS3VTVVMQTEGF5**

- **25072003-1188.jpg** Y6VAO5CQRCRLZY6NMA2TA6C4OA2QDQFU
- **25072003-1118.jpg** XLLSMJTIYDY5LGE4FNGXA2HWOGS3JT3K
- **25072003-1170.jpg** 5P5YDMAKOSRK4LUC72GQQMSIIOKRCGWM
- **23012005-188.jpg** USAKWPUB7Y7ZN6URGZEPADSCWLCO7SUI
- **23012005-202.jpg** SUMGX3FNWG3RUUZK5POHH53VE2ALVDL6
- **25072003-1138.jpg** HAP3Q3YJWU5PVPRQCHUJW7NDMWK7KF3Q
- **25072003-1099.jpg** ZM3ZZ7YBLBZWGNNYJ6XRPF5SNH46JBMK
- **25072003-1187.jpg** JP7GJJPCOZ4CAHZZK4KVTAGA4OGWQWRA
- **sandra5.jpg** UH3XYN6SGV6TMGE54XICUKKXIUIEZPRL
- **sandra model full frontal-stan222000.jpg** 56UHB2TVLFGLOEUWGJF4QQIUSC7JK4EN
- **23012005-203.jpg** XGAZFORQN2PVZWWESCRVP3RNOEMAPUJH
- **25072003-1168.jpg** 6D3VTWP6HLJSQK6Z2U2NWB5TRMRKE4PW
- **25072003-1117.jpg** K2624L3R6KLOWHM5RI24JIHZP2VKCB7Z
- **25072003-1093.jpg** 6M2SDK42UE47NSNFHCRZBR3T7SIPXI4I
- **25072003-1121.jpg** ARK774Y5ABXO7DKHJFXSW5OYFJAK2NNZ
- **25072003-1125.jpg** WYM67ENAXNBJHSZ6J7NGTGKNMZK23BZI
- **25072003-1156.jpg** C55P2PHSYWNEMXPYE6SSUVNFM2OAV42V
- **25072003-1134.jpg** 6JA4UQDK2N2LK3MNSEHPCKHCFV5KYQ6V
- **25072003-1104.jpg** AAEBXBUYVWLGOEUZMTZI6F2J65A4DENC
- **25072003-1167.jpg** OLDBJYJ33EN3MPBL2J5EOYZKAOIIZ6XW
- **25072003-1151.jpg** VOU23NFCMV6ZC3ERZFSEFQQE74S2KQH3
- **Sandra-mix-57.jpg** VHDF4VWM5HYZ3HZPCITT2SSO4QDQKGD2
- **25072003-1175.jpg** WEZGGZTDSPOCEK7M3MJOU4L74ZX3WQI
- **25072003-1169.jpg** GN7FNA4QK7WWOP4OTWWLDRY64HGTL4SV
- **23012005-178.jpg** KOAQOPIXKHROT7PKEOPOX7NOA2TFGNE6
- **25072003-1100.jpg** YMGMGY5XXB2OJYDPVUDEFIGCP6FIP63K
- **25072003-1101.jpg** ZSFV4N44YWKSDAU5BDYIH45L4GR6E3GA
- **23012005-437.jpg** 55MGRNJPAZALAPKQ25HMRPOQKWSQEC5L
- **25072003-1096.jpg** 564ZLWDSN455Y4GRZENCSBUO6Y4IP2HY
- **Sandra-mix-46.jpg** B6ACNVVWD43V3ZENQSCMDUGADUA6H2YQ
- **25072003-1112.jpg** QMVCIXSTRRUOJBA5E2FRCQHV6752RUCC
- **23012005-206.jpg** ZRXSDJJN322V24VJXOZRCBKMKB6RFRJ5
- **25072003-1177.jpg** WCFCR7W7SWR6GNKDIZ65DR774UJTP4D6
- **25072003-1107.jpg** A5MEBEM7O35UPEPQWHFQ6BYZPBNR6NKU
- **23012005-442.jpg** VQTGZCB5K5CCAMKV6RU4LPVOT2VQ3FG6
- **04112004-1418.jpg** IOEGJZZ6MWNZIA3NLNFMRSPMIIK7ET5I
- **23012005-307.jpg** LCAT5Q7JGSXEM7BVMDVTVY2ZNM5FIONZ
- **25072003-1174.jpg** Q5WQVTT63TZBZOXMXM4WUBTDW3KUHDOQ
- **s5.jpg** Q5WQVTT63TZBZOXMXM4WUBTDW3KUHDOQ
- **23012005-499.jpg** 4Z24T2NCYZNSC2WSC4VENQ73PMA4YGAN
- **25072003-1113.jpg** V4GGFODNZBOZO646CN7PIPE2D2RET6JY
- **25072003-1153.jpg** 2XBUEKJX76PN4PKRM2YKY37RNMSE6ZSY
- **25072003-1166.jpg** OHTCWI4Y5D55JCAGXN6APNB7DXHHM7YS

- **25072003-1106.jpg** 42Z3CO3M3UD4S7UGOJW3LL3PL7MJLOIY
- **25072003-1157.jpg** FMV3KN7AGY6J7F4XIUTCINMWN3PJ6C5O
- **23012005-179.jpg** QCVH4HIYO7KHM7QM3AKMNIIIT2HMIWVM
- **25072003-1097.jpg** 6K3ILEUGVADXN5ZTIYGGDFDWOWPLOEK2
- **25072003-1111.jpg** 67N74O3RV7V3FB4CKHMYJ5EBNXOJOLCA
- **23012005-293.jpg** S7MDCQU5CNSRCZD7YLM2XFSB43BFKEMA
- **25072003-1186.jpg** PP747ISWWUQNP2ZT4T24U5TNUG5RUA57
- **25072003-1114.jpg** NWHNUX3XFE32JI2IYUYUHI3WETICHIRM
- **Sandra-mix-26.jpg** 663GIYBP7DCYCHW5YTWBZP6CS5X3H2QB
- **23012005-180.jpg** EHC6SSMWMYY34YAZPW22Y5YRZAZCDSTR
- **25072003-1110.jpg** QV2TMK3VDG53UFDF2HH5VNRYJYUWFX3N
- **23012005-176.jpg** NG5AP4QTDBXF32EP5GUZPJFRISOESELJ
- **25072003-1150.jpg** UG4DZWTKD2E3YH7AI36DJDED55LYWFPP
- **25072003-1098.jpg** VJ2HCPM3OF3GTEX4GGQQ4D4QBUGE4VQK
- **25072003-1149.jpg** L4WSR63U5DCVULOW5QT6YHQR6UA4QB4L
- **23012005-279.jpg** 44W6Y7LECLXIZLMOZV4XBFH3V74F7LJF
- **25072003-1135.jpg** PCHK5SBVL6ZHWUUKBJO3SZWHIYODP3EF
- **s4.jpg** C5PYALCOJJJPTXHYZIFUTXJ3X4YL36UC
- **25072003-1179.jpg** C5PYALCOJJJPTXHYZIFUTXJ3X4YL36UC
- **s26.jpg** WNMBUP5RTKEGCZGFRGU56TMOMHXO2ZKZ
- **Sandra Teen Model Nude 00014.jpg** RZY6ODGZVUSO4MRS63IEDFUGRK4KYXSK
- **25072003-1136.jpg** BUPV3MVXNWAGOQP27IYDW3JMCOXSFEQD
- **23012005-443.jpg** IWDTCYFK5I5XQ36PN3M4JMS7W7EN7LSJ
- **25072003-1124.jpg** PRSKQI23C5P5BUHZTDVGPYJ47OMVOYB6
- **IMG_4142.jpg** XS7E6KCSMLMYJRH6BBBVDB7WEUH7OLYA
- **25072003-1085.jpg** DPBSHC7KDCEDL4I3CM66DIHB3FYVXJ74
- **IMG_4547.JPG** JW55HDSR7NVYIM57VBPGR2BQ4Q4FHJLW
- **23012005-214.jpg** P6JRNAZUPYRX25PAC5GNKX46JMOQADXG
- **25072003-1142.jpg** FL5YN5NKAUDA64SVHOR2LD4EICUQNQSA
- **Sandra-mix-60.jpg** RN6NSFYTLZSZG45QPYODZBIBA5WGCUNS
- **25072003-1137.jpg** RRS2CRZV6OE3QZWGQL2R6IOGPM4L4SYL
- **Sandra-mix-49.jpg** 5B7NPL46LGLXPYHVDBH7YAEYOFCA4O46
- **25072003-1091.jpg** 5INRKXD4V3A5IFA5TS6B5KCXCPV3BOWL
- **sandra2.jpg** ZWYXPB2GHWBSNJNRKYHEEHU2SKN6APTW
- **25072003-1119.jpg** BA2CXJPXSITU5YEZUVCBKHNMUII6QUUK
- **Sandra-mix-08.jpg** IEZN7KNJYWRGB6QYLFFA2NKTWMXT2P5B
- **25072003-1161.jpg** J2P2G3XACUP37SUIV5GBYKVBHDSMOCOS
- **25072003-1089.jpg** XKUMQHXCWBE6IOSDSSDUZVGKSHGUCMW6
- **Sandra-mix-25.jpg** INDP6Z73ZXAQYOEBCYOFCZYXN3HF4ASV
- **25072003-1102.jpg** WPBLK6CYMQNSMVKLXSOAG2VFW2HSBCUZ
- **25072003-1160.jpg** N4OCI6I4FOMFJGZRUWCHX7SZY6YUFIGC
- **25072003-1158.jpg** MBUSP4RKDX33XC2VBKGFECYJOXVCMSMS
- **25072003-1140.jpg** GFB25RCZKEDNXWDPBFEESLLLOZRDZSSE

- **Sandra Teen Model Nude 00007(1).jpg**
  MS6A5P7UZUI3EHVWRWG7J3F2A7LFOS3Q
- **25072003-1088.jpg ISFB5XZTXSULGHQRVR7ARL47YQSKYK2G**
- **25072003-1103.jpg YJZTHXTX7X53YAYMQGWTAQPWJ7AE3DS4**
- **25072003-1147.jpg W66VDIFD3MBM7GADR63Y3ONGPUCIT72Y**
- **25072003-1090.jpg V6PHLPHEBINIY5O3VGUYSJR5IU75TTDI**
- **Sandra-mix-28.jpg RPNOG5L4ETNPKA3CNKJZJME7XH5D7PNB**
- **ptsc Sandra Teen Model 00011 Nude underwater small pics (1).jpg**
  EAQSYUIEFNVYAWYNGZCEAPK2Z6EFP25I
- **sandra3.jpg IXM6JMRNBHL3C32DNTSRIK5QEERF3FHM**
- **25072003-1139.jpg EX7C4WBIWI43EDA55Z2JXERE7ZAU3R3O**
- **Sandra-mix-23.jpg AFHR4C7VDD2QE37JE6YSMHD6KJB4RPS7**
- **25072003-1122.jpg 5TJLJHE4QMC5CP3SS2ZSV3QZFGQTZTAY**
- **s23.jpg 7PMXANEQ32B7S4OZCJRFTARUNEG3H4WV**
- **25072003-1105.jpg 53TGKOAWYVJWZZ5DY6V2YFUBUBVQH47F**
- **Sandra-mix-15.jpg YP5SORONGGUGMBIGKYKLDTTW6KDTBTWF**
- **Sandra-mix-17.jpg E4PPNPEZ4FOKF6E3HQLV4BMX5PSMCQRU**
- **25072003-1159.jpg XKJXTAY7U4XQKNZMREGLXUI5OEVELP4K**
- **Sandra-mix-27.jpg 2DMI3GLQXN3CX7VHEWIMJOF7QGVCBFI5**
- **Sandra-mix-21.jpg FH4H2Y7PPNCQP6P3VVCI7HH72UERQMBX**
- **25072003-1162.jpg BW4GKU32V4L3OFP2DQ5RIIIVJ4XWBE34**
- **Sandra-mix-54.jpg CT3SHONPWEMB63HLHAITSPDPETVVHX7D**
- **Sandra-mix-55.jpg 3R4AWM43LUC4ZXH7NZ737L4Y6NGSBK7W**
- **Sandra Teen Model Nude 00017.jpg**
  FZCS7CUC7JTOQY2JN2VQJ6JNTDBRSTVW
- **1111274542.jpg 6LBHRKBO2VZBCK3XAVZFCOOITWEZSTV5**
- **s20.jpg ICAUEQR7NT2LHW4HAJK5CEFM57XIGXYS**
- **Sandra-mix-16.jpg QXMA2POEKN5V3AO2BGWLWEEOTM23TV56**
- **25072003-1145.jpg ZT4IMGRSDQSVA5YM43D2MQHZDJQLE5U6**
- **25072003-1144.jpg HCX36SNMEQFWW55N4LKPGE2F642MIFO5**
- **SANDRA_MIX_60.jp HVOVQHDIXW7EUWZMGUYDV7UI3JBVLZIW**
- **Sandra-mix-51.jpg LVOB57PAWQZOMPC6ZZFHHQWKRU5RQBTO**
- **s18.jpg GFW6IREFKRHLKZ5GALAVLMCAHO7KRMU5**
- **25072003-1143.jpg 4D2I2WEKNYT6YZKHOZ2N3BWFELGMESTZ**
- **s21.jpg IGAJKRH7PNLCMKHSGFLIZSIQAVQJ3LV3**
- **s7.jpg HEZWCNGDRAEVWPUXCDE5PQIIGJ77REUB**
- **s17.jpg HBGKFPGYBT56RBRXQHVBUNJGLTTAXBTQ**
- **Sandra nude.jpg TW4SRJ34LATYOZA4JNHKF25OVW7E7FQE**
- **25072003-1146.jpg QGV6YS35734W3Y7ESJE3IQXLBP347IRW**
- **s16.jpg 75YCJYX3YJX4VN4AKJ6AXCJJWQSA6VH5**
- **Sandra-mix-52.jpg PQ42LDC4TRZ24I7VILTKQU5JC4VK7B6O**
- **Sandra-mix-61.jpg I3RWTZ5U63SCJHPI4HXY7HVD5ZNBN7A3**
- **Sandra74_jpg.jpg IK3GY7DGOM6GV3Z36Y7KNNELOLWGLWPY**

SA Pena then looked through the file structure of InfoHash: **ebac972f542da319c737e96c43bae9d50b3784e3** and observed that in the folder titled: "**Sandra Model (Misc nude)**". Which is where the above listed 152 "Files of Interest" are located. Some of these files were complete or incomplete and some of these files could be considered "Child Erotica" and "Child Pornography".

SA Pena reviewed the above listed downloaded .jpg files and some are described as follows:

- **25072003-1157.jpg (SHA1: FMV3KN7AGY6J7F4XIUTCINMWN3PJ6C5O) (Located Inside Folder: Sandra Model (Misc nude))** This color .jpg image file depicts a naked pre-pubescent female in an outdoor setting and crawling away from the camera on her hands and knees in water. The camera is focused on the young girl's vaginal area; with the main focus point of the image her vagina. The young girl's vagina, anus and buttocks are visible. This girl appears to be between 8 and 11 years of age, due to her body size comparison/development and no pubic development.

- **25072003-1170.jpg (SHA1: 5P5YDMAKOSRK4LUC72GQQMSIIOKRCGWM) (Located Inside Folder: Sandra Model (Misc nude))** This color .jpg image file depicts a naked pre-pubescent female in an outdoor setting and standing in a stream. The young girl is shown from her chin area to her knees and she is facing the camera. The young girl's vagina and breast area are visible. The girl has her legs slightly apart. The main focal point of the image is a close-up of the young girl's vagina. This girl appears to be between 8 and 11 years of age, due to her body size comparison/development, very slight/budding breast development and no pubic development.

- **25072003-1174.jpg & s5.jpg (SHA1: Q5WQVTT63TZBZOXMXM4WUBTDW3KUHDOQ) (Located Inside Folder: Sandra Model (Misc nude))** This color .jpg image file depicts a naked pre-pubescent female in an outdoor setting, beside trees and rocks. The girl is shown from her chin area to her knees and she is facing the camera. The young girl has her arms folded across her breast area. The young girl's vagina area is visible. The girl has her legs slightly apart. The focal point of the image is a close-up of the young girl's vagina. This girl appears to be between 8 and 11 years of age, due to her body size comparison/development, no apparent breast development and no pubic development.

Possessing and distributing these files does constitute a violation of the Sexual Exploitation of Children federal statue Title 18, United States Code, Section 2252 and all of these files are considered child pornography.

On November 18, 2014, SA Pena was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **b4dc3c7c5031aacfc9c22c84c588b14794356cae**. This torrent file references 774 files, at least one of which was identified as being a file of investigative interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116**, hereinafter referred to as "Suspect Device." The Suspect Device reported it was using BitTorrent client software **-BA3300- uTorrent 3.3**.

On November 18, 2014, between 2118 hours and 2314 hours MST, SA Pena successfully completed the download of 9 file(s) that the device at IP address **174.56.57.116** was making available. The device at IP Address **174.56.57.116** was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

- **t-002-028.jpg** **LQ35T4S6IURQNKZ7O7MAPC24LMEMFT4T**
- **t-002-057.jpg** **2RJ4UQKYUJ4TPOXSXXNTYFF5E3Q4VQAE**
- **t-002-066.jpg** **OHIZNQ2O4TEPXFUU3DDQYLLTBXASDZDN**
- **t-002-067.jpg** **3H6NGPNMWKSYJRWHZKBNYQIPJL3CA7W4**
- **ism-016-057.jpg** **WQK6OTE22DNAEEKH52RVGRVTG5TZ4HVQ**
- **ism-016-098.jpg** **GTBP3Z52ABHVBFNTRJQ7VE5QJU7G4DPJ**
- **touch-005a-052.jpg** **3I4NEQSOT3HSBG7ONKDQWFTCSHAYVV7D**
- **isa-024-103.jpg** **2HXK44AO5XZ7PF6S254DCANS3IXHTYNF**
- **lsh-003-101.jpg** **6B24QJRT47BXPW62TSMVBWM7YIG4J3OW**

SA Pena then looked through the file structure of InfoHash: **b4dc3c7c5031aacfc9c22c84c588b14794356cae** and observed in the folder titled: "LS FairyLand Stunning Dolls etc [6 sets 2 Vids] FotoSketcher+LS-Art " inside this folder were subfolders: "FotoSketcher + LS Art (by me with this program)", "LS FairyLand 002", "LS FairyLand 005", "LS Island-03-Midsummer_ism-016", "LS Touch 005a", "Ls-Island.Issue.02-In-The-Middle.24", "LS-Land issue 21 Stunning Dolls Set 03", and multiple .jpg/.avi files, which is the location of the above listed 9 files of interest. Some of these files were complete or incomplete and some of these files could be considered "Child Erotica" and "Child Pornography."

SA Pena reviewed the above listed downloaded .jpg files and some are described as follows:

- **ism-016-057.jpg (SHA1: WQK6OTE22DNAEEKH52RVGRVTG5TZ4HVQ) (Located Inside Folder: LS Island-03-Midsummer_ism-016)** This color .jpg image file depicts a naked pre-pubescent female in an outside setting and climbing on a rock. She has a multi-colored scarf tied around her waist. Her leg is high up on the rock exposing her vaginal area for the camera. Her breast area and buttocks are exposed. She is looking over her shoulder and smiling at the camera. In the upper left corner of the image is the logo: "LS island." This girl appeared to be between 8 and 10 years of age, due to her body size comparison/development, no breast development and no pubic development.

- **t-002-066.jpg (SHA1: OHIZNQ2O4TEPXFUU3DDQYLLTBXASDZDN) (Located Inside Folder: LS FairyLand 002)** This color .jpg image file depicts a naked pubescent female in a studio setting and posed in a lewd or lascivious manner. The girl is wearing a hat and a small piece of green cloth around her neck. Her right leg is placed high upon a multi-colored object that resembles a flower. The way the girl is posed her vaginal area is visible to the camera. The young girl's breasts and buttocks are also visible. In the upper right corner of the image are the logos: "LS MODELS.COM" and "http://www.ls-

models.com." This girl appears to be between 11 and 12 years of age, due to her body size comparison/development, no breast development and slight pubic development.

- **isa-024-103.jpg (SHA1: 2HXK44AO5XZ7PF6S254DCANS3IXHTYNF) (Located Inside Folder: Ls-Island.Issue.02-In-The-Middle.24)** This color .jpg image file depicts a naked pre-pubescent female sitting in an outside setting and sitting on rocks or pebbles. The girl is shown from her lower chest to her lower thigh area. She has her legs spread far apart and the focal point of the close-up image is her vagina and anus. In the upper right corner of the image is the logo" LS island." This girl appears to be between 8 and 11 years old, due to her body size comparison/development and no pubic development.

Possessing and distributing these files does constitute a violation of the Sexual Exploitation of Children federal statue Title 18, United States Code, Section 2252 and all of these files are considered child pornography.

JANUARY 2015

On January 1, 2015, SA Pena was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **f6b14881b75fdd7fa4a91f09784ecd88edd670da**. This torrent file referenced one file, which was identified as a file of interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116**, hereinafter referred to as "Suspect Device." The Suspect Device reported it was using BitTorrent client software -**BA3300- uTorrent 3.3**.

On January 1, 2015, between 0320 hours and 0411 hours MST, SA Pena successfully completed the download of the following file that the device at IP address **174.56.57.116** was making available. The device at IP Address **174.56.57.116** was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

- **14 yr young girl begs for sex (only for trades).mpg**
  Y44RD7AGAON5CFUD3D2WJ4HKWMBNWILS

SA Pena then looked through the file structure of InfoHash:
f6b14881b75fdd7fa4a91f09784ecd88edd670da and observed that inside this torrent is where the above listed one "Files of Interest" is located.

SA Pena reviewed the above listed downloaded .mpg file and it is described as follows:

- **14 yr young girl begs for sex (only for trades).mpg (SHA1: Y44RD7AGAON5CFUD3D2WJ4HKWMBNWILS)** This video or movie is 4 minutes and 58 seconds in length. This video depicts a pubescent female seated on a bed with an adult male. The adult male is touching the girl's legs and breasts through her clothing. It shows the girl undressing in front of the male. The video then shows the adult male naked

on the bed while the girl masturbates his penis and performs oral sex on his penis. The adult male is seen penetrating the young girl's vagina with his penis and using his penis to touch her breasts. The adult male appears to ejaculate on her stomach at the end of the video. This girl appears to be between 13 and 15 years of age, due to her body size comparison/development, her apparent breast development and her pubic development.

Possessing and distributing these files does constitute a violation of the Sexual Exploitation of Children federal statue Title 18, United States Code, Section 2252 and all of these files are considered child pornography.

FEBRUARY 2015

On February 3, 2015, SA Pena was conducting an online investigation on the BitTorrent network for offenders sharing child pornography. SA Pena directed his investigative focus to a device at IP address **174.56.57.116 (Port: 6881)**, because it was associated with a torrent with the InfoHash: **f9a32fe27d06e875db077b7e1ef9cb86e0d32d46**. This torrent file referenced one file, which was identified as being a file of interest to child pornography investigations.

Using a computer running investigative BitTorrent software, SA Pena directly connected to the device at IP address **174.56.57.116,** hereinafter referred to as "Suspect Device". The Suspect Device reported it was using BitTorrent client software **-BA3300- uTorrent 3.3**.

On February 3, 2015, between 2205 hours and 2215 hours MST, SA Pena successfully completed the download of the following 1 file(s) that the device at IP address **174.56.57.116** was making available. The device at IP Address **174.56.57.116** was the sole candidate for each download, and as such, each file was downloaded directly from this IP Address.

- **LS-magazine-Issue 19 911(3000FOTO).jpg**
  3365M2HH4KLGJA7DBLPZVX6IMDIYIYQU

SA Pena then looked through the file structure of InfoHash:
f9a32fe27d06e875db077b7e1ef9cb86e0d32d46 and observed that inside this torrent is where the above listed 1 "Files of Interest" is located.

SA Pena reviewed the above listed downloaded .jpg file and it is described as follows:

- **LS-magazine-Issue 19 911(3000FOTO).jpg (SHA1: 3365M2HH4KLGJA7DBLPZVX6IMDIYIYQU)** This color .jpg image file depicts a capture of a web site with the following caption: "911 This One Contains 30 Collections 3000 Photos 100 Pics In Each Set" and the following URL: http://rghost.ru/users/opus87/releases/link1, "pass lolita888." Also on this web site capture were two pre-pubescent females in a studio setting, posing in a lewd and lascivious manner. The dark haired girl was naked from the waist down and her buttocks were visible. The blonde haired girl was completely dressed and has her legs spread apart, so the side of her vaginal area is visible. This image file could be considered "Child

Erotica". These girls appeared to be between 8 and 12 years of age, due to body size comparison/development and no apparent breast development.

Possessing and distributing these files does constitute a violation of the Sexual Exploitation of Children federal statue Title 18, United States Code, Section 2252 and all of these files are considered child pornography.

On February 18, 2015, SA Pena conducted a query on the IP address **174.56.57.116** through the American Registry for Internet Numbers (ARIN). ARIN reported IP address **174.56.57.116** to be registered to Comcast Cable Communications, Inc.

On February 18, 2015, at or about 1300 hours MST, SA Pena obtained a Grand Jury Subpoena Duces Tecum from the 2nd Judicial District for Comcast Cable and for IP address **174.56.57.116**; with the assistance of Assistant Attorney General Tony Long.

On February 19, 2015: SA Pena received sought after information from Comcast Cable, who responded back with the subscriber information for IP Address **174.56.57.116** and which showed the subscriber information as follows:

Subscriber Name: **Marcella Johnson**
Service Address: 3958 Montgomery Blvd NE-Apt #101, Albuquerque, NM, 87109
Telephone #: 505-903-0346
Start of Service: Unknown
E-mail User IDs: marcellajohnson3337@comcast.net
MAC Address: e8:89:2c:4f:1f:12
IP Address History: 174.56.57.116
Account Status: Active
IP Assignment: Dynamically Assigned

SA Pena then placed all of the BitTorrent download evidence artifacts from RoundUp BitTorrent on a disc for SA Melva Boling (Homeland Security Investigations, Albuquerque, NM), due to IP Address **174.56.57.116** being located within Bernalillo County. This case was completely turned over to SA Boling (HSI).

On March 2, 2015, Affiant began conducting surveillance at 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109, locating the residence and confirming its location. Your Affiant has conducted surveillance on the residence on numerous occasions since March 2, 2015. The license plate tags of cars parked in front of the apartment have been identified through investigative systems as being registered to Marcella Johnson and/or Michelle Johnson. Your Affiant observed a female leaving the identified apartment and entering a red Pontiac four-door car with New Mexico license plate 736SNA, which is registered to Bobby or Nancy Johnson of Cuba, New Mexico. Your affiant compared the woman to a photo from the Department of Motor Vehicles and believes that woman to be Marcella Johnson. The same red Pontiac has been present in front of the apartment consistently since March. The last surveillance was conducted on June 1, 2015 and the identified red Pontiac was still present. Also

present was a 2011 Ford Mustang, New Mexico license plate 860RZK, which is registered to Marcella and Michelle Johnson.

Your Affiant knows that Homeland Security Investigations and the New Mexico Internet Crimes Against Children Task Force Affiliates have executed numerous search warrants using the techniques described in this investigation. In prior cases the suspect confessed and/or the materials/computers were seized and found to contain evidence confirming the undercover operation related to child pornography.

COMPUTERS AND COMPUTER RELATED MEDIA INVOLVED IN CHILD PORNOGRAPHY

Your Affiant knows that computer files or remnants of such files on computers and computer related media can be recovered months or even years after they have been downloaded, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a computer and/or computer related media, the data contained in the file does not actually disappear; rather, that data remains on the media until it is overwritten by new data. The actual file is not initially erased or removed from the computer and/or computer related media, but rather, it remains available in free space on the computer and/or computer related media until overwritten by other information. The "deleted" file can also be overwritten by information when the computer user takes a positive action to permanently remove the "deleted" file from the hard drive, such as employing "wiping" software, formatting the hard drive, or de-fragmenting or compressing the information located on the hard drive. However, "deleted" files which have not yet been overwritten by other information can often be successfully recovered during the search of a computer system or computer related media. These "deleted" files are often recovered long after the date the criminal activity occurred. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

Your Affiant knows that computer hardware consists of all equipment that can collect, analyze, create, display, convert, store, conceal or transmit electronic, magnetic, optical or similar computer impulses or data. Hardware includes any data processing devices such as central processing units, memory typewriters and self-contained "laptop" or "notebook" computers, internal storage devices such as fixed hard disks, floppy disk drives and diskettes, magnetic tape drives and tapes, optical storage devices, and other memory storage devices, as further described in Attachment B, incorporated herein by reference. Some computer hardware can be internal to the computer system or external. The external component hardware is often referred to as peripheral and includes input/output devices such as keyboards, printers, scanners, plotters, video display monitors and optical readers, web cameras, communication devices such as modems, recording equipment, RAM or ROM units, automatic dialers, video/digital camera equipment, flash drives, thumb drives, key drives, USB devices, removable/portable hard drives,

media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media.

Your Affiant knows cameras, both digital and still, and video recording equipment have capabilities of capturing images of evidentiary value. In addition, a digital camera is capable of allowing the user to view images transferred from a computer via external media, such as a media card, or directly downloaded from the computer to the camera's internal memory.

Your Affiant knows that computers and computer related media's ability to store images in digital form makes them an ideal repository for child pornography. A single DVD, CD-ROM, jump drive, hard drive, thumb drive, compact flash, other memory cards and other devices (as referenced in Attachment B) can store thousands of images and hundreds of thousands of pages of text, with storage capacities increasing all of the time. The size of the fixed electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the past several years. Hard drives with a capacity of one hundred gigabytes or more are not uncommon. These drives can store hundreds of thousands of images at a very high resolution. Electronic storage located in host computers adds another remote dimension to this storage equation.

Your Affiant knows that computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical or other digital form. It commonly includes programs to run operating systems, applications such as word processing, graphics or spreadsheet programs, utilities, compilers, interpreters and communications programs.

Your Affiant knows computer passwords and data security devices are designed to restrict access to, or hide, computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password, a string of alpha-numeric and/or special characters, usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips and circuit boards. Data security software or digital codes may include programming code that creates "test" or "hot" keys that perform pre-set functions when depressed. "Hot" keys can be designed to erase, or otherwise render unusable, data contained within computer memory storage devices.

Your Affiant knows documents can be created using computer software programs, and those documents can be used to facilitate the commission of crimes. In some cases, mere possession of certain types of documents constitutes criminal conduct. Computer systems can also store information in internal or peripheral storage devices including fixed disks, floppy diskettes, tape drives, optical storage devices or other memory storage devices such as flash drives, thumb drives, key drives, USB devices, IPods, IPads, PSP Players, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media. Based on my training and experience, and my use of computer systems in my employment as a Special Agent, I know users of computer systems

often save information or create documents and save them to various types of computer-related storage devices, both internally, such as the hard drive, and externally, such as a thumb drive.

Your Affiant knows that computers are expensive and that people keep them in their possession for several years. Even after people buy a new computer they often do not dispose of their old computer. It is common for people to possess old computers for several years either because they do not want to dispose of an item that was expensive or because they do not know how to delete the personal information they have accrued on their computer.

Your Affiant knows from training and experience, and training and experience of other law enforcement personnel to whom your Affiant has spoken, that those persons who possess, trade, receive or distribute images of minors engaged in sexually explicit conduct view children as sexual objects, and such persons receive gratification from sexually explicit images of minors.

Your Affiant knows from training and experience that persons who possess, trade, receive, or distribute sexually explicit images of minors often maintain their sexually explicit images of minors, and such images can include all types of media such as still photographs, digital photographs, video clips, digital video clips, printouts, magazines, and videotapes. From training and the training and experience of other agents to whom your Affiant has spoken, many individuals interested in child pornography have admitted being addicted to the images and find sexual gratification in said images. Your Affiant knows that currently the most prevalent media used is digital media, including digital photographs and digital video clips that are stored on the possessor's computer hard drive, computer diskettes, CD ROM's, and various external computer memory storage devices, such as flash drives, thumb drives, key drives, USB devices, IPods, IPads, tablets, PSP Players, gaming systems, removable/portable hard drives, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), CDs, DVDs, Blu-ray discs, minidiscs, other optical disks, and other external media, some of which can be extremely small and stored easily in personal safes, lockboxes, vehicles, or on one's person. Additionally, your Affiant knows from training and experience that digital images are easily printable in "hard copy" form and can be stored virtually anywhere inside a residence, vehicle, boat, garage, sheds, bank safety deposit boxes, lock boxes, and personally owned safes, as well as other areas under the control of those persons possessing, distributing, and receiving sexually explicit images of minors.

Further, your Affiant knows digital media storage devices including "thumb drives," "flash drives", "pen drives", or memory sticks are by their very nature designed to be small enough to carry in one's pocket or affixed to a key chain. Also, your Affiant is aware that digital cameras and video recording devices contain storage disks that are like "thumb drives," in that they can hold large quantities of data, and come in very small sizes. Your Affiant knows that such storage devices are able to store digital images, and by their nature are extremely portable and can easily be concealed on one's person or in one's clothing.

Your Affiant knows that many cellular telephones and Personal Digital Assistants (PDA's) are capable of receiving, distributing and possessing child pornography images through infrared transmissions as a picture message or attachment to a text message sent to or received from other cellular telephones, PDA's, and computers. Many models of cellular telephones and

PDA's have two storage capabilities. The device may have built-in memory capable of holding child pornography images and also utilize removable storage options capable of holding child pornography images (such as compact flash cards, secure digital cards, and memory sticks). Many of these storage cards are capable of being read by computers, other cellular telephones, PDA's, and can be loaded directly onto printers.

Your Affiant knows through training and experience, and the training and experience of other law enforcement officers, that those persons who possess, receive, and distribute sexually explicit images involving minors often use digital media such as digital still cameras and digital video recorders to capture and upload such sexually explicit images, including photographing said images that appear on a computer screen. Your Affiant also knows through training and experience and the training and experience of other agents that standard 35mm cameras and film are used to capture sexually explicit images.

Your Affiant knows through training and experience that undeveloped 35mm film located within residences being searched for images depicting sexually explicit conduct by minors is considered evidentiary in nature. Your Affiant knows the seizure and processing, including the development, is essential in determining the presence of further evidence.

Your Affiant knows that persons seeking to possess, distribute, and receive sexually explicit images of minors most often use the Internet to do so. The Internet is a worldwide network that connects computers and allows communication and transfer of data, information, and images across state and national boundaries. Individuals who use the Internet can communicate electronically by using e-mail. E-mail messages can contain text, data, and images. This type of communication is private in that it is directed from one Internet user to another. Internet users can also communicate using chat rooms and instant messaging. Both chat rooms and instant messaging incorporate "real time" communication between Internet users. Instant messaging, like e-mail, is private, in that it is one Internet user communicating specifically, and exclusively, with another. Internet Service Providers such as America Online (AOL), and web sites such as Yahoo! provide software and venue for such one to one contact. The Internet offers a number of facilities which allow users to access, distribute, and exchange information including the World Wide Web (WWW), File Transfer Protocol (FTP), electronic e-mail (E-mail), and postings on newsgroups. The WWW allows users to display and access data in a multimedia format. FTP is a method of distributing and receiving files between computer systems. A newsgroup is an Internet site that is devoted to a particular area of interest or discussion including child pornography. Users may send or post messages and responses to be read at any time by others, much like a bulletin board.

Evidence of distribution, receipt, and possession of child pornography is often found on the user's computer and other computer media. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer and other media used in connection with child pornography. Storing this information can be intentional, i.e., by saving an e-mail as a file or saving the location of one's favorite websites for example, bookmarked files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or Internet Service Provider client software, among others). Additionally, a

computer user's Internet activities generally leave traces or footprints in the web cache and history files of the browser used. A forensic examiner can often recover evidence of child pornography in this intentionally and unintentionally retained digital information.

Your Affiant knows through training and experience that connecting to the Internet can be done from standard dial-up telephone lines, Digital Subscriber Lines (DSL), Cable Modem lines, and Local Area Networks (LAN). Connection logs provided by ISP's allow investigators to establish times, dates, and in some instances locations from where the connections were made.

Your Affiant knows through training and experience that digital evidence, including registry file and other data may exist on computers that can be used to prove the identity of those who use the computer and computer related media and their possible involvement with visual depictions of minors engaged in sexually explicit conduct.

Your Affiant knows through training and experience that individuals who show an interest in visual depictions of minors engaged in sexually explicit conduct may have in their possession journals, correspondence, and other writings detailing their and other's involvement with visual depictions of minors engaged in sexually explicit conduct or a sexual interest in children. Your Affiant knows these individuals may also keep records related to their internet service provider and internet services.

Based upon the foregoing, your Affiant thus believes there is probable cause to believe that visual depictions of minors engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2252 exist at the residential property and premises located at 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109.

III. INTERSTATE NEXUS

Individuals who utilize P2P file sharing client programs, such as ARES, must connect to the Internet to share files with other individuals. In order to access the Internet and P2P file-sharing programs, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. Your Affiant believes that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. 2252 and for the limited purpose of securing a search warrant.

For purposes of possession only, under 18 U.S.C. 2252 (a) (4) (b) the Government can show the images were produced by an item manufactured outside New Mexico. HSI computer forensics examiner Special Agent Kyle Craig stated to your Affiant that he is unaware of any computer hardware/digital media capable of holding data being manufactured in the state of New Mexico, other than the Intel processors produced at the Intel facility in Rio Rancho, NM. Intel processors contain on-chip cache memory that is volatile and not conducive for transporting stored data, not to be confused with hard drives, flash drives, or other non-volatile digital media that maintains the data after power is removed.

IV. SEARCH AND SEIZURE

Your Affiant knows based upon training, experience, and information relayed by law enforcement officers and others involved in the forensic examination of computers that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips as described in Attachment B. Searches and seizures of computers and computer-related media requires agents to seize all computers and computer-related media described in Attachment B to be processed by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

A. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are many types of computer hardware and software in use today, so it is impossible to bring to the search site all necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system being searched.

B. Searching computer systems requires the use of precise scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

C. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises.

D. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

In order to search for data that is capable of being read or interpreted by a computer and computer-related media described in Attachment B, law enforcement personnel will need to

search, seize, image, copy, and examine the following items believed to be evidence and/or an instrumentality of a violation of 18 U.S.C. 2252, subject to the procedures set forth above:

A. All computer equipment and storage device which are capable of being used to commit or further the crimes outlined above, or create, access or store the types of evidence, fruits, or instrumentalities of such crimes as outlined in Attachment B;

B. All computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners which are capable of being used to commit or further the crimes outlined above, or create, access or store the types of evidence, fruits, or instrumentalities of such crimes as outlined in Attachment B;

C. All magnetic, electronic or optical storage devices capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic notebooks, cellular telephones, digital cameras, video cameras (both digital and analog), thumb drives, memory sticks, USB flash drives, key drives, USB devices, media cards (including xD-Picture cards, Multi Media cards, Compact Flash cards, Memory Sticks, Secure Digital Cards, Solid State drives), IPods, IPads, tablets, PSP players, gaming systems, printers, scanners, video game systems, Blu-ray discs, minidiscs, removable/portable hard drives, magnetic tapes, Video Home System tapes (VHS), ZIP drives and personal digital assistants capable of being used to commit or further the crimes outlined above, or create, access or store the types of evidence, fruits, or instrumentalities of such crimes as outlined in Attachment B;

D. All documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software.

E. All applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

F. All internet service provider records;

G. All physical keys, encryption devices, dongles, and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

H. All passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

I. Writing tablets, journals, correspondence and other written content evidence that may identify individual involvement.

CONCLUSION

Based on the information set forth above, there is probable cause to believe that computer(s) and computer related media described in Attachment B, which are located on the apartment and premises described in Attachment A, are instrumentalities and evidence of the sexual exploitation of minors, in violation Title 18 U.S.C. 2252, and should be seized as such. Furthermore, based upon the foregoing paragraphs, judicial authority is specifically requested to search for and seize computer equipment, storage devices, video equipment, and other evidence outlined in Attachment B, and complete the search/examination of the seized computers and computer related media at an appropriate law enforcement facility.

WHEREFORE, I respectfully request that a warrant be issued authorizing Homeland Security Investigations, with appropriate assistance from other law enforcement officers, to enter said premises, and search for, seize, and examine the items set forth above and in Attachment B.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge. FURTHER AFFIANT SAYETH NOT.

Special Agent Melva Boling
Department of Homeland Security
Homeland Security Investigations

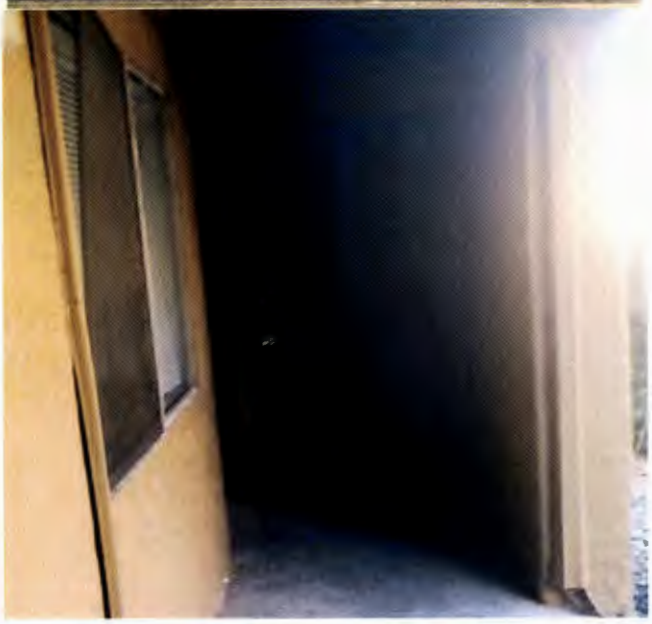
Subscribed and sworn before me this 10 day of June, 2015

The Honorable Kirtan Khalsa
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The premises to be searched are described as the residential property and premises located at 3958 Montgomery Boulevard NE, Apartment 101, Albuquerque, New Mexico 87109. The property is an apartment complex named the Canyon Vista Apartments. The building is brown in color and has windows facing the west. Apartment 101 is located on the west side of the building on the bottom floor. The apartment entry faces the east and "101" is affixed to the door.



ATTACHMENT B

ITEMS TO BE SEARCHED FOR AND SEIZED

1. All electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, cellular telephones, PDAs, IPods, IPads, Tablets, gaming systems or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers and related communication devices such as modems; together with system documentation, operating logs and documentation, software and instruction manuals, handwritten notes, logs, user names and lists.

2. All of the records below, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, electronic address books, calculators or any other storage media, together with indicia of use, ownership, possession or control of such records.

3. Any photographs, digital images, videos, computerized graphic files, printed material, computer images or files made by electronic or mechanical means which are located on the premises which show a person who is or depicted as being under the age of eighteen years engaged in or depicted as being engaged in sexual conduct or the lewd exhibition of the genitals.

4. All books, magazines, documents, advertisements portraying children under the age of eighteen engaged in sexual conduct, posed in sexually explicit positions or that contains unclothed or partially unclothed children under the age of eighteen.

5. All materials or items which are sexually arousing to individuals who are interested in minors, but which are not in and of themselves obscene or which do not necessarily depict minors involved in sexually explicit conduct. Such material is commonly known as "child erotica" and includes written materials, written communications and emails, personal journals dealing with child development, sex education, child pornography, sexual abuse of children, incest, child prostitution, investigative techniques of child exploitation, sexual disorders, pedophilia, diaries, and fantasy writings.

6. All documents tending to show occupancy ~~and/or ownership of the home~~ of the apartment 101 KK ME, including personal identification, bills, receipts, canceled mail, utility bills, rent receipts and bank statements.

7. All documents including e-mail to or from the occupants of the residence or documents relating to account(s) with any online services, bills, receipts, canceled checks, bank statements, applications and advertisements.

8. All diaries, logs, notations, telephone/address books, telephone answering machine tapes, correspondence, e-mail, chat conversation and/or any other documentation tending to show

any communication or correspondence with any companies or person supplying, distributing or trading in child sexual abuse materials, or sexual conduct with minors.

9. All financial records, telephone records, correspondence, ledgers or other documents showing the purchase and/or sale of images of child sexual abuse material.

10. All electronic equipment, projectors, televisions, VCR's and/or any other device, that will be needed to watch, playback an item that was seized.

11. All lockboxes, and locked containers located inside apartment 101. KK MB ~~, vehicles, and outlying structures located on the property or curtilage.~~

12. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

13. Search all persons present inside the apartment (search only, not seize).

14. Red pontiac four-door car with New Mexico license plate 736SNA and 2011 Ford Mustang with New Mexico license plate 860RZK if located on the property at the time of the search. (search only, not seize). KK MB